

# PATENT ABSTRACTS OF JAPAN

③

(11)Publication number : 2001-057554

(43)Date of publication of application : 27.02.2001

(51)Int.Cl.

H04L 12/24  
H04L 12/26  
H04L 12/46  
H04L 12/28  
H04L 12/66  
H04L 12/56

(21)Application number : 11-265942

(71)Applicant : BABA YOSHIMI

(22)Date of filing : 17.08.1999

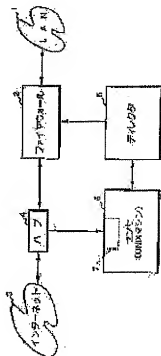
(72)Inventor : BABA YOSHIMI

## (54) CRACKER MONITOR SYSTEM

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a cracker monitor system that can automatically detect an attack from a cracker on a network and protect the network from the attack by the cracker in spite of a simple system configuration without limiting the communication as required or over and the need for a labor by a skillful engineer.

**SOLUTION:** An entrance of a LAN 1 is provided with a sensor 5 that sequentially acquires an IP packet passing through the entrance. The sensor 5 senses various attacks from a cracker with respect to the LAN 1 on the basis of the acquired IP packet. Information with respect to the attacker sensed by the sensor 5 is given to a director 6 controlling a firewall 2. The director 6 controls the setting of the firewall 2 in response to the given information to block the IP packet relating to the sensed attack from entering the LAN 1.



(Partial Translation)

JP 2001-057554 A

- 5 [Embodiment of the invention]  
[0008] An embodiment according to the present invention is explained with reference to Fig. 1. Fig. 1 is a diagram of a system configuration according to the present embodiment. In Fig. 1, numeral 1 is a LAN as a network.
- 10 The LAN 1 is architected with, for example, Ethernet, and a plurality of hosts (computers) (not shown) are connected via an Ethernet cable, hub, and the like. An Ethernet card for connecting to the Ethernet cable, software for performing TCP/IP processing, various application software
- 15 that run on the TCP/IP (for example, telnet, ftp, and smtp) are implemented in each of the hosts, enabling communication based upon the IP. The LAN 1 is not limited to the architected network on the Ethernet, however any architecture mode such as token ring and the like can be
- 20 employed. In the system according to the present embodiment, a computer 2 having a function of a firewall as a packet filter (hereinafter, simply "firewall 2 for the computer 2") is arranged at an entrance for the LAN1. The LAN1 is connected to an internet 3 via the firewall 2. The
- 25 firewall 2 has a file (hereinafter, "filter setting file") in which data is written for defining what type of IP packet is prohibited for entering into the LAN 1. When the type of the IP packet that is prohibited for entering into the LAN 1 is sent from a side of the internet 3 by the
- 30 filter setting file, the IP packet is discarded to block the entry into the LAN 1. When the IP packet that is not prohibited for entering into the LAN 1 is sent by the filter setting file, the IP packet is transferred to the LAN 1. A hub 4 is mounted between the firewall 2 and the

internet 3, and a sensor 5 having a function as an attack detecting unit is connected to the hub 4. Furthermore, a director 6 having a function as a processing unit that controls the firewall 2 is connected to the sensor 5. The sensor 5 and the director 6 are respectively configured with a computer. The sensor 5 is, for example, configured with an NIX machine and connected to the hub 4 via the Ethernet card 7. In this case, software called TCP DUMP is implemented in the sensor 5. The TCP DUMP enables acquiring (hearing) all IP packets that pass through the hub 4 via the Ethernet card 7. The sensor 5 stores and retains each of the acquired IP packets and the time data indicative of time at which the IP packet is acquired in hard disk (not shown). If the total number of the IP packets stored in the hard disk reaches the predetermined allowable capacity, the sensor 5 deletes the oldest IP packet to store newly acquired IP packet in the hard disk. Furthermore, the sensor 5 does not have an IP address and can receive (load) only the IP packet by setting the software not to be responsive to the response-requesting packet to be sent such as ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol), and the like. Moreover, software (hereinafter, "attack detecting algorithm") for detecting the first to sixth type attacks mentioned above are implemented in the sensor 5. The attack detecting algorithm can be implemented in the director 6 allowing the sensor 5 to perform processing the attack detecting algorithm while sending and receiving data to and from the director 6. Software (hereinafter, "filter control algorithm") that controls the firewall 2 is implemented in the director 6. In this case, the filter control algorithm rewrites the date of the filter setting file depending upon the attack detected by the sensor 5 to control the firewall 2. Next, operation according to the

present embodiment is explained. The sensor 5 performs the following processing per predetermined cycle time while storing the acquired IP packet in the hard disk. That is, a plurality of the IP packets for the predetermined time

5 interval are classified (sorted) per value of source IP address and value of destination IP address to be loaded into a memory (not shown). In other words, out of the IP packets for the predetermined time interval, the IP packets having the identical source IP address are consolidated and

10 the IP packets having the identical destination IP address are consolidated to be loaded into the memory (hereinafter, a consolidated set of the IP packets is referred to as "IP packet group"). A plurality of the IP packets loaded into the memory are processed for attack detection that is

15 mentioned later and then the IP packets are deleted from the memory. In this case, the IP packets to be loaded into the memory are IP packets that are acquired after predetermined time elapses since acquiring the oldest IP packet in the IP packets loaded into the memory in the

20 previous cycle time. The processing for attack detection by the sensor 5 in each cycle time is performed in the following manner based upon the attack detection algorithm. The sensor 5 processes detecting, for example, the first type attack out of the first to sixth attacks, namely port

25 scanning. In this processing, for each IP packet group that has the identical source IP address and the source IP address is for an external from the LAN 1 in the IP packets loaded into the memory as described above, the sensor 5 extracts value (IP address value belonging to LAN 1) for

30 all the destination IP addresses held by the IP packets that are included in the each IP packet group. Thereafter, for each value for the destination IP address extracted in the above each IP packet group, the sensor 5 counts the number of the IP packets that are acquired in predetermined

continuous time (for example, within 30 seconds), and that have the identical destination IP address to the value for the above destination IP address from the IP packet group (IP packet group of the identical source IP address) having

5 different destination port number in the TCP header or the UDP header. When the counted number reaches the predetermined number (for example, 20), the sensor 5 detects attacking of port scanning and sends the data indicative of the attack together with value data

10 (hereinafter, "first type attack detection data") for the source IP address of the IP packet group on which the attack is detected to the director 6. Such processing is performed sequentially for all IP packet groups having the identical source IP address that does not belong to LAN 1.

15 In the present embodiment, detection of port scanning is performed by counting the number of the IP packets having different port numbers, however the detection of port scanning can be performed by the following processing. Namely, for each IP packet group having the identical

20 source IP address and the source IP address is for an external from the LAN 1, by extracting value for all the destination port numbers held by the IP packets that are included in the each IP packet group, the number of the IP packets that are acquired within predetermined continuous

25 time and that have the identical destination port number to the value for the above destination port number and have different destination IP addresses is counted from the IP packet group with the extracted destination port number with respective to each value of the extracted destination

30 port number. When the counted number reaches the predetermined number, port scanning is detected. On the other hand, the director 6 that is provided with the first type attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry of

the IP packets that have the identical source IP address to the source IP address included in the first type attack detection data for predetermined time (for example, for five minutes) from the present time. In this time, upon  
5 receiving the IP packets having the source IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of port scanning. If the director 6 is again provided with the first type attack  
10 detection data identical to the first type attack detection data that is previously provided before predetermined time (five minutes) elapses, the director 6 controls the firewall 2 to block the entry of the IP packets from the source IP address of the first type attack detection data  
15 into the LAN 1. Accordingly, unless attacking of port scanning continues, the IP packets from the source IP address cannot enter into the LAN 1. If the director 6 is not provided with the first type attack detection data again within the predetermined time (five minutes),  
20 blocking of the entry into the LAN 1 by the IP packets from the IP source address of the first type attack detection data is released. In this manner, after the sensor 5 completes processing for detecting an attack of port scanning, the sensor 5 performs processing for second type  
25 attack detection (SYN FLOOD). In this processing, for the IP groups having the identical destination IP address, the sensor 5 sequentially extracts the IP packets for SYN included in the each IP packet group having the destination IP address that belongs to LAN 1 in chronological order of  
30 acquiring thereof. Thereafter, the sensor 5 checks whether the IP packets for SYN acquired within predetermined time (for example, 2 seconds) from the time acquiring the extracted IP packets for each SYN present in the IP packet group having the identical destination address. In case of

presence, the sensor 5 counts the number of the IP packets for SYN including the previously extracted IP packets for SYN. Moreover, for the counted IP packets for SYN, the sensor 5 checks whether the IP packets for ACK

5 corresponding to respective IP packets for SYN (IP packets for ACK having the identical source IP address to that for the IP packets for the SYN, and having the next sequence number to the sequence number in the TCP header for the IP packets for the SYN) that are acquired within the

10 predetermined time (2 seconds) from the time for acquiring the IP packets for the SYN present in the IP packet group having the identical destination address. In case of presence, the number of the counts is decremented by one for every time. If the count is equal to or greater than

15 the predetermined number (for example, 16) at the time of finally completing checking of the presence of the corresponding IP packets for ACK, an attack of SYN FLOOD is detected and the data indicative of such attack and the value data for the source IP address and the value data for

20 the destination IP address (hereinafter, "second type attack detection data") of the IP packets for SYN for which the attack is detected are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that

25 belongs to LAN 1. In the present embodiment, detection of SYN FLOOD is performed based upon the number of the IP packets for SYN, however the detection of SYN FLOOD can be performed by the following processing. Namely, for each IP packet group having the identical source IP address that

30 belongs to the LAN 1, IP packets for SYN/ACK included in the IP packet group are extracted in chronological order of acquiring thereof. Thereafter, the sensor 5 checks whether the IP packets for SYN/ACK acquired within the predetermined time (for example, 2 seconds) from the time

of acquiring the extracted IP packets for each SYN/ACK present in the IP packet group having the identical source address. In case of presence, the sensor 5 counts the number of the IP packets for SYN/ACK including the

5 previously extracted IP packets for SYN/ACK. Moreover, for the respective IP packets for SYN/ACK, the sensor 5 checks the IP packet group having the identical destination address to that for the source IP address for presence of the IP packets for ACK corresponding to the IP packets for

10 the SYN/ACK (IP packets or ACK having the identical destination IP address to the source address for the IP packets for the SYN/ACK, and having the next ACK number to the sequence number in the TCP header for the IP packets for the SYN/ACK) that are acquired within the predetermined

15 time (2 seconds) from the time for acquiring the IP packets for the SYN/ACK present in the IP packet group. If such packets for ACK present, the number of the counts is decremented by one for every time. If the count is equal to or greater than the predetermined number (for example,

20 16) at the time of finally completing checking of the presence of the corresponding IP packets for ACK, an attack of SYN FLOOD is detected. In this case, the data to be provided to the director 6 from the sensor 5 are the data indicative of detection of the attack of SYN FLOOD, the

25 value data for the source IP address and the value data for the destination IP address of the IP packets for the SYN/ACK. In this case, the value data for the source IP address and the value data for the destination IP address of the IP packets for SYN/ACK respectively correspond to

30 the value data for the source IP address and the value data for the destination IP address of the IP packets for SYN in the aforementioned second type attack detection data. The director 6 that is provided with the second type attack detection data from the sensor 5 rewrites the filter

setting file of the firewall 2 to block the entry of the IP packets having the identical source IP address to the source IP address included in the second type attack detection data for predetermined time (for example, for two minutes) from the present time. Simultaneously, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets having the identical destination IP address to the destination IP address included in the second type attack detection data for predetermined time (for example, for two minutes) from the present time. In this time, upon receiving the IP packets having the source IP address or the IP packets having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of SYN FLOOD and the host having the attacking target IP address can be resumed to the normal state without shutting down. Similarly to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the second type attack detection data identical to the second type attack detection data that is previously provided before predetermined time (two minutes) elapses for eliminating the IP packets having the source IP address in the second type attack detection data, the director 6 controls the firewall 2 to block the entry of the IP packets from the source IP address of the second type attack detection data into the LAN 1. The same can be applied to elimination of the IP packets having the destination IP address in the second type attack detection data. Accordingly, unless attacking of SYN FLOOD continues, the IP packets from the source IP address associated with the attack or the IP packets from the destination IP address associated with the attack cannot enter into the LAN 1. For elimination of any one of the IP packets having

the source IP address in the second type attack detection data or the IP packets having the destination IP address in the second type attack detection data, if the second type attack detection data is not provided to the director 6

5 before the each corresponding predetermined time (for two minutes and for two seconds) elapses, blocking of the entry into the LAN 1 by the IP packets having the source IP address of the second attack detection data or IP packets having the destination IP address of the second attack

10 detection data is released. In this manner, the sensor 5 that completes processing detection of the attack of SYN FLOOD proceeds to processing detection of the third type attack (Teardrop). In this processing, the sensor 5 sequentially extracts IP packets that are split

15 (hereinafter, simply "split packets") and that are included in the each IP packet group having the identical destination IP address that belongs to the LAN 1. In this case, in IP, a certain flag in the IP header is one or the data that is so-called fragment offset has larger value

20 than zero for the split packets, whereby the split packets can be found. The sensor 5 checks for presence of packets in the IP packet group identical to the split packets that are acquired within the predetermined time (for example, in five minutes) from the time of acquiring the extracted each

25 split packets and the fragment offset value and the IP identification number in the IP header are identical to those for the split packets (split packets identical to the extracted split packets). If such split packets present, the sensor 5 counts the number of the split packets

30 including the previously extracted split packets. If the count is equal to or greater than the predetermined number (for example, 80), an attack of Teardrop is detected and the data indicative of the attack, the value data for the source IP address of the split packets and the value data

for the destination IP address (hereinafter, "third attack detection data") of the IP packets for which the attack is detected are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the third attack detection data from the sensor 5 controls the firewall 2 in the same manner as the case for detecting the SYN FLOOD. In other words, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets having the identical source IP address to the source IP address included in the third type attack detection data into the LAN 1 for predetermined time (for two minutes) from the present time. Simultaneously, the director 6 rewrites the filter setting file of the firewall 2 to block the entry of the IP packets that have the identical destination IP address to the destination IP address included in the third type attack detection data for predetermined time (for two minutes) from the present time, whereby the LAN 1 is protected from the attack of Treardrop and the host having the attacking target IP address can be resumed to the normal state without shutting down. In this manner, after the sensor 5 completes processing for detecting an attack of Treardrop, the sensor 5 performs processing for fourth type attack detection (LAND). In this processing, from the each IP packet group having the destination IP address that belongs to the LAN 1 in the IP packet groups having the identical destination IP address, the sensor 5 extracts IP packets having the source IP address identical to the value for the destination IP address in the IP packet group. Furthermore, the sensor 5 checks for presence of the IP packets that are acquired within the predetermined time (for example, in two minutes) from the time of acquiring the IP packets and that have the

identical source IP address to that for the IP packets in the IP packet group having the destination IP address identical to that for the extracted IP packets. If such IP packets present, the number of the IP packets including the previously extracted IP packets is counted. If the count is equal to or greater than the predetermined number (for example, 6), an attack of LAND is detected and the data indicative of the attack, the value data for the source IP address of the IP packets for which the attack is detected (hereinafter, "fourth attack detection data") are provided to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the fourth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets that have the identical source IP address to the source IP address included in the fourth type attack detection data and that have the identical destination IP address to the source IP address for predetermined time (for example, for five minutes) from the present time. At this time, upon receiving the IP packets having the source IP address and the IP packets having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the attack of LAND. Similarly, to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the fourth type attack detection data identical to the fourth type attack detection data that is previously provided before the predetermined time (five minutes) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to the source IP address in the fourth type attack detection data, the director 6

controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fourth attack detection data for the predetermined time (for five minutes) from the moment that the director 6 is provided with the fourth attack detection data. Accordingly, unless attacking of LAND continues, the IP packets having the source IP address and the destination IP address associated with attacking cannot enter into the LAN 1. If the fourth attack detection data is not provided, the director 6 releases the blocking of the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address identical to the source IP address of the fourth attack detection data.

[0009] In the present embodiment, the value data for the source IP address of the IP packets associated with the attack of LAND is made to be provided to the director 6 as the fourth attack detection data. Because the source IP address has the same value as that for the destination IP address of the IP packets associated with the attack of LAN, alternatively for the value data for the source IP address, the value for the destination IP address can be provided to the director 6. As mentioned above, after the sensor 5 completes processing for detecting the attack of LAND, the sensor 5 performs processing for fifth type attack detection (acquiring password). In this processing, for the IP groups having the identical destination IP address, the sensor 5 extracts IP packets that include the user name data and the password data for the host of the LAN 1 for the each IP packet group having the destination IP address that belongs to the LAN 1. The sensor 5 counts the number of the IP packets acquired within a predetermined continuous time (for example, within two minutes) having the identical user name data and different password data

from the extracted IP packets. When the counted number is equal to or greater than the predetermined number (for example, 20), the sensor 5 detects a fifth type attack for acquiring a password and sends the data indicative of the attack together with the value data for the source IP address and the value data for the destination IP address (hereinafter, "fifth type attack detection data") of the IP packets for which the attack is detected to the director 6. Such processing is performed sequentially for all IP packet groups having the identical destination IP address that belongs to LAN 1. The director 6 that is provided with the fifth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets that have the source IP address and the destination IP address identical to the fifth type attack detection data for predetermined time (for example, for one hour) from the present time. At this time, upon receiving the IP packets having the source IP address or having the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the fifth type attack aiming at acquiring the password. Similarly to the case for detecting port scanning, if the director 6 is again provided by the sensor 5 with the fifth type attack detection data identical to the fifth type attack detection data that is previously provided before predetermined time (one hour) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to those in the fifth type attack detection data, the director 6 controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fifth attack detection data for the

predetermined time (one hour) from the moment that the director 6 is provided with the fifth attack detection data. Accordingly, unless the fifth type attack continues, the IP packets having the source IP address and the destination IP address associated with the attacking cannot enter into the LAN 1. If the director 6 is not provided with the fifth type attack detection data again before the predetermined time (one hour) elapses, blocking of the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address of the fifth type attack detection data is released. In this manner, after the sensor 5 completes processing for detecting the attack of LAND, the sensor 5 performs processing for sixth type attack detection (attacking through hole). In the processing, for the IP packet groups having the identical destination IP address, the sensor 5 retrieves IP packets having, for example, "lpr" command as the printer logical name with a data size being equal to or greater than 128 characters for the each IP packet group having the destination IP address that belongs to LAN 1. If such IP packets are retrieved, the sixth type attacking on the through hole of the host of LAN 1 is detected, and the data indicative of the attack, the value data for the source IP address and the value data for the destination IP address of the IP packets for which the attack is detected (hereinafter, "sixth attack detection data") are provided to the director 6. The director 6 that is provided with the sixth attack detection data from the sensor 5 rewrites the filter setting file of the firewall 2 to block the entry into the LAN 1 by the IP packets having the source IP address and the destination IP address identical to the source IP address and the destination IP address of the sixth type attack detection data for predetermined time (for example, for six hours) from the present time. At this time, upon receiving the IP

packets having the source IP address or the destination IP address from the internet 3, the firewall 2 discards the IP packets to block the entry thereof into the LAN 1, whereby the LAN 1 is protected from the sixth type attack on the

5 through hole of the host of the LAN 1. Similarly to the case for detecting port scanning, if the director 6 is again provided with the sixth type attack detection data identical to the sixth type attack detection data that is previously provided from the sensor 5 before the

10 predetermined time (six hours) elapses for eliminating the IP packets having the source IP address and the destination IP address identical to those in the sixth type attack detection data, the director 6 controls the firewall 2 to block the entry into the LAN 1 by the IP packets having the

15 source IP address and the destination IP address of the sixth attack detection data for the predetermined time (six hours) from the moment that the director 6 is provided with the sixth attack detection data. Accordingly, unless the sixth type attack continues, the IP packets having the

20 source IP address and the destination IP address associated with the attacking cannot enter into the LAN 1. If the director 6 is not provided with the sixth type attack detection data again before the predetermined time (six hours) elapses, blocking of the entry into the LAN 1 by the

25 IP packets having the source IP address and the destination IP address of the sixth type attack detection data is released. As explained above, according to the system of the present embodiment, only introducing the sensor 5 and the director 6 enables real-time detection of various

30 attacks on the LAN 1 by crackers and taking appropriate countermeasure promptly and automatically to protect the LAN 1 from the detected attack, thereby extensively reducing workload for a network administrator such as establishing the LAN 1 considering an attack by a cracker

or frequently referring a log file, leading to reduction of the management cost for the LAN 1. Furthermore, various attacks by the crackers can be detected in real time, so that in the state that no attack is detected, necessity for

5 restricting communication between the LAN 1 and the external can be reduced, whereby the degree of freedom for communication by the LAN 1 in the normal state can be enhanced and the information resource on the internet 3 is effectively utilized. In the embodiment explained above,

10 by providing the firewall 2 in the entrance for the LAN 1 and controlling the firewall 2 when detecting an attack by a cracker, the detected attack is automatically eliminated. Alternatively, when detecting the attack by the cracker, the processing can be simply performed such that the attack

15 is notified to the network administrator, an expert security administrator, and the like. In this case, for example, the director 6 or the sensor 5 is connected to the host for the network administrator, the expert security administrator, or the like via a public line or an

20 exclusive line. If detecting an attack, the information such as the first to sixth attack detection data are sent to the host for the network administrator, the expert security administrator, and the like from the director 6 or the sensor 5. If configured in this manner, the specific

25 countermeasure for protecting the LAN 1 from the detected attack is taken directly by the network administrator or the like. In this case also, the network administrator or the like can take the countermeasure when notified. Moreover, the type of the attack is detected, so that the

30 countermeasure against the attack can be taken relatively easily.

[Brief description of the drawings]

[Fig. 1] A diagram of a system configuration of a cracker

monitoring system according to an embodiment of the present invention.

[Description of the numerals]

- 5 1 LAN (network)
- 2 Firewall (packet filter)
- 3 Internet
- 4 Hub
- 5 Sensor (attack detecting unit)
- 10 6 Director (processing unit)
- 7 Ethernet card



## 【特許請求の範囲】

【請求項1】 IP (Internet Protocol) 1) に基づく通信を行うネットワークの入り口において該入り口を通過するIPパケットを逐次取得し、取得したIPパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするクラッカー監視システム。

【請求項2】 前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのIPパケットを受信可能に構成されていることを特徴とする請求項1記載のクラッカー監視システム。

【請求項3】 前記攻撃検知手段は、IPパケットの受信のみが可能に構成されていることを特徴とする請求項2記載のクラッカー監視システム。

【請求項4】 前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得したIPパケットから前記アルゴリズムに基づき各種類の攻撃を検知することを特徴とする請求項1〜3のいずれか1項に記載のクラッカー監視システム。

【請求項5】 前記攻撃検知手段は、所定時間内に取得した複数のIPパケットを少なくとも送信元IPアドレス及び/又は宛先IPアドレスにより分類して保持する手段を具備し、その分類したIPパケットから前記各種類の攻撃を検知することを特徴とする請求項4記載のクラッカー監視システム。

【請求項6】 前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のIPパケットであって、少なくともその送信元IPアドレスが互いに同一で且つ宛先IPアドレス又は宛先ポート番号が互いに異なるものが所定時間内に所定数以上取得されたとき、第1の種類の前記攻撃がなされたことを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項7】 前記攻撃検知手段は、前記ネットワークにその外部から送信されてきたTCP (Transmission Control Protocol) に基づく複数のSYN用IPパケットであって、少なくともその宛先IPアドレスが互いに同一であるものが所定時間内に所定数以上取得され、且つ、その各SYN用IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有すると共に前記TCPに基づくACK用IPパケットが前記所定時間内に取得されなかったとき、第2の種類の前記攻撃がなされたことを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項8】 前記攻撃検知手段は、前記ネットワークからその外部に送信されたTCP (Transmission

Control Protocol) に基づく複数のSYN/ACK用IPパケットであって、少なくともその送信元IPアドレスがそれぞれ互いに同一であるものが所定時間内に所定数以上取得され、且つ、前記TCPに基づくACK用IPパケットであって、前記各SYN/ACK用IPパケットの送信元IPアドレス及び宛先IPアドレスとそれぞれ同一の宛先IPアドレス及び送信元IPアドレスを有するものが前記所定時間内に取得されなかったとき、第2の種類の前記攻撃がなされたことを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項9】 前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数の分割されたIPパケットであって、同一の分割部分が所定時間内に所定数個以上取得されたとき、第3の種類の前記攻撃がなされていることを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項10】 前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のIPパケットであって、その送信元IPアドレスが宛先IPアドレスと同一のアドレスとなっているものが所定時間内に所定数個以上取得されたとき、第4の種類の前記攻撃がなされていることを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項11】 前記攻撃検知手段は、前記ネットワーク内の特定のホストを操作する該ネットワークにその外部から送信されてきた複数のIPパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定時間内に所定数以上取得されたとき、第5の種類の前記攻撃がなされていることを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項12】 前記攻撃検知手段は、バッファオーバーフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するIPパケットを取得したとき、第6の種類の前記攻撃がなされていることを検知することを特徴とする請求項1〜5のいずれか1項に記載のクラッカー監視システム。

【請求項13】 前記処理手段が行う処理は、前記攻撃が検知された旨を表す報知出力を発生する処理であることを特徴とする請求項1〜12のいずれか1項に記載のクラッカー監視システム。

【請求項14】 前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元IPアドレス及び/又は宛先IPアドレスを有するIPパケットの前記ネットワークへの進入を阻止する処理であることを特徴とする請求項1〜12の記載のクラッカー監視システム。

【請求項15】 前記処理手段が行う処理は、前記攻撃検知手段が前記第1の種類の攻撃を検知してから所定時

間、前記攻撃検知手段が検出した前記第1の種類の攻撃に係る前記送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項6記載のクラッカー監視システム。

【請求項16】前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項7記載のクラッカー監視システム。

【請求項17】前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項16記載のクラッカー監視システム。

【請求項18】前記各SYN用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理は、前記各SYN用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項17記載のクラッカー監視システム。

【請求項19】前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項8記載のクラッカー監視システム。

【請求項20】前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN/ACK用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項19記載のクラッカー監視システム。

【請求項21】前記各SYN/ACK用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記各SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項20記載のクラッカー監視システム。

【請求項22】前記処理手段が行う処理は、前記攻撃検知手段が前記第3の種類の攻撃を検知してから所定時間、前記分割されたIPパケットに係る宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットが前

記ネットワークに進入するのを阻止する処理であることを特徴とする請求項9記載のクラッカー監視システム。

【請求項23】前記処理手段が行う処理は、前記攻撃検知手段が前記第3の種類の攻撃を検知してから所定時間、前記分割されたIPパケットに係る送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含むことを特徴とする請求項22記載のクラッカー監視システム。

【請求項24】前記分割されたIPパケットに係る送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記分割されたIPパケットに係る宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定されていることを特徴とする請求項23記載のクラッカー監視システム。

【請求項25】前記処理手段が行う処理は、前記攻撃検知手段が前記第4の種類の攻撃を検知してから所定時間、該第4の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項10記載のクラッカー監視システム。

【請求項26】前記処理手段が行う処理は、前記攻撃検知手段が前記第5の種類の攻撃を検知してから所定時間、該第5の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項11記載のクラッカー監視システム。

【請求項27】前記処理手段が行う処理は、前記攻撃検知手段が前記第6の種類の攻撃を検知してから所定時間、該第6の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理であることを特徴とする請求項12記載のクラッカー監視システム。

【請求項28】前記ネットワークの入り口には、該ネットワークに進入を阻止するIPパケットを選択的に設定可能なパケットフィルタが設けられ、前記処理手段は、前記処理を該パケットフィルタを制御することにより行うことを特徴とする請求項14～27のいずれか1項に記載のクラッカー監視システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

【0002】本発明は、クラッカーによるネットワークへの攻撃を監視し、さらにはその攻撃からネットワークを保護するためのシステムに関する。

## 【従来の技術】

【0003】近年、企業などの組織内に構築されたネットワーク（LAN）は、その多くがインターネットに接続され、他のネットワーク等との間での各種情報のやりとり（通信）がインターネットを介して行われている。この通信では、一般に、所謂OS I階層モデルにおけるネットワーク層に対応するプロトコルとしてIP（Internet Protocol）が用いられ、通信データはIPパケットの形態でやりとりされる。そして、上記ネットワーク層の上位のトランスポート層に対応するプロトコル（IPの上位のプロトコル）として、TCP（Transmission Control Protocol）あるいはUDP（User Datagram Protocol）を用いるのが通例である。この種のネットワークは、インターネット上のサーバや他のネットワークなどとの間で、多種多様な情報のやりとりを低コストで行うことができるという利点を有する反面、インターネットが極めて高度な公開性を有することから、所謂クラッカーからの攻撃を受ける危険性にさらされることとなる。このため、そのような攻撃からネットワークを保護することが要求される。このようなネットワークの保護を行うためのシステムとしては、従来、保護しようとするネットワークの入り口に、ファイアウォール（詳しくはファイアウォールの機能をもたせたコンピュータ）を設けたシステムが知られている。このファイアウォールは、あらかじめネットワーク管理者などがネットワーク内への進入を阻止すべきものとして定めた種類の通信データ（IPパケット）がネットワーク内に進入するのを阻止し、それ以外の許可された通信データのみを通過させるパケットフィルタとして機能するものである。この場合、ネットワーク内への進入を阻止する通信データの種類は、例えばIPパケットに含まれる送信元IPアドレスや宛先IPアドレス、宛先ポート番号などによって指定可能とされている。このようなファイアウォールによれば、ネットワーク内の特定のIPアドレスを有するホスト（コンピュータ）、あるいはそのホストの特定のポート番号に対する外部からのアクセスを禁止したり、ネットワークの外部の特定のIPアドレス以外のIPアドレスからのネットワークへのアクセスを禁止したりすることができる。従って、ネットワークへの進入を禁止する通信データの種類のファイアウォールに対して適切に設定しておけば、ネットワークへの攻撃の危険性を低減することが可能である。しかしながら、この種のファイアウォールでは、その設定を適切に行うためには、通信技術やネットワーク技術、クラッカーによる攻撃手法など、ネットワークに関連した幅広い範囲の技術に対する高度の知識と理解が必要であると共に、個々のネットワークの構造や運用形態についても熟知している必要がある。つまり、ファイアウォールにより阻止する通信データの種類の、それにより保護しよ

うとするネットワークの各ホストがどのような情報を利用し、もしくは外部に提供し、また、ネットワーク内のどのような情報を保護すべきか、予想される攻撃としてどのようなものが想定されるか、ということなどを総合的に考慮して決定しなければならず、このためには、ネットワーク関連の高度な熟練技術者を要する。そして、特に保護しようとするネットワークの規模が比較的大きい場合や、該ネットワークで扱う情報が多岐にわたるような場合には、熟練技術者といえども、ファイアウォールの適切な設定を行うことは困難である。さらに、ネットワークの構成を変更したような場合や、クラッカーからの攻撃を実際に受けたような場合、あるいは新たな手法の攻撃が出現したような場合には、多くの場合、ファイアウォールの設定内容を構築し直す必要があり、ファイアウォールを含めたシステムの継続的な運営管理が必要となる。従って、ファイアウォールの設定や、その管理運営には、熟練技術者による多大な労力やコストを要するものとなっていた。また、上記のような従来のファイアウォールは、攻撃の可能性のある通信をすべて排除しようとするものであり、設定により禁止された種類の通信は、その通信がクラッカーからの攻撃によるものであるか否かにかかわらず一律的に排除される。つまり、ネットワークと外部との通信の自由度が必要以上に制限される。このため、ファイアウォールを備えたネットワークでは、インターネット上の利用可能な情報提供サービスの制限を受け、インターネット上の多くの情報資源を有効に享受することができないという不都合を生じるものであった。

## 【発明が解決しようとする課題】

【0004】本発明はかかる背景に鑑みてなされたものであり、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による努力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができるクラッカー監視システムを提供することを目的とする。

## 【課題を解決するための手段】

【0005】本発明のクラッカー監視システムは、かかる目的を達成するために、IP（Internet Protocol）に基づく通信を行うネットワークの入り口において該入り口を通過するIPパケットを逐次取得し、取得したIPパケットを監視することにより該ネットワークに対するクラッカーからの攻撃を検知する攻撃検知手段と、該攻撃検知手段が前記攻撃を検知したとき、それに応じた所定の処理を行う処理手段とを備えたことを特徴とするものである。すなわち、本発明者等がクラッカーによる各種攻撃の手法を検討したところ、多くの種類の攻撃は、そのそれぞれがIPパケット内のデータやIPパケットの通信形態に特徴がある。従って、前記ネットワークの入り口でそこを通過するIPパ

ケットを前記攻撃検知手段によって逐次取得し、その取得したIPパケットを監視することで、クラッカーによる前記ネットワークへの攻撃をリアルタイムで検知することができる。そして、このように攻撃を検知できれば、それに応じて前記処理手段により適当な処理（例えばネットワーク管理者などの報知や、クラッカーによる通信を遮断する処理等）を行うことで、その攻撃からのネットワークの保護を図ることができる。この場合、クラッカーによる攻撃が十分に進行するまでには、一般に長い時間を要するため、攻撃が検知された時点、あるいは、それから若干遅れた時点でネットワークを保護するための処置を行っても、ネットワークの損害を十分に抑えることができる。このような本発明のシステムによれば、クラッカーによる攻撃をリアルタイムで検知できるため、その検知がなされたときに攻撃に対する対策処置を施せばよい。このため、ネットワーク管理者等は、所謂ログファイル（通信記録簿）等を頻繁に参照したりする必要性が低減されると共に、ネットワークの構築や再編等の際に、クラッカーによる攻撃を予測的に考慮するような努力が軽減される。また、攻撃が検知されない通常時は、ネットワークとその外部との通信を、攻撃の可能性を予測して制限する必要性がなく、その通信の自由度を高めることができる。従って、本発明によれば、ネットワークに対するクラッカーからの攻撃を自動的に検知し、通信を必要以上に制限したり、熟練技術者による努力を必要とすることなく、簡易なシステム構成でクラッカーからの攻撃に対するネットワークの保護を図ることができる。かかる本発明においては、前記攻撃検知手段は、前記ネットワークの入り口を通過する全てのIPパケットを受信可能に構成しておく。これにより、クラッカーによる多くの種類の攻撃を速やかに検知することが可能となる。さらに、本発明では、前記攻撃検知手段は、IPパケットの受信のみが可能に構成しておく。これによれば、前記攻撃検知手段は、自己のIPアドレスやMAC（Media Access Control）アドレス等、自己情報のデータをネットワークに送信することがないため、クラッカーなどによりその存在が認識されたり、攻撃の対象とされることがない。従って、攻撃検知手段の安全性を確保し、ひいては、本発明のシステムの信頼性を確保することができる。また、本発明では、前記攻撃検知手段は、複数の種類の前記攻撃に対して、各種類の攻撃を検知するためのアルゴリズムを保持しており、取得したIPパケットから前記アルゴリズムに基づき各種類の攻撃を検知する。これにより、クラッカーによる複数の種類の攻撃を検知することが可能となり、前記ネットワークの安全性を高めることができる。また、前記アルゴリズムを適宜更新することで、新しい種類の攻撃に対しても対応することが可能となる。この場合、前記攻撃検知手段は、所定時間内に取得した複数のIPパケットを少なくとも送信元IPアドレ

ス及び/又は宛先IPアドレスにより分類して保持する手段を具備し、その分類したIPパケットから前記各種類の攻撃を検知する。すなわち、複数の種類の攻撃を検知するためには、IPパケットの送信元IPアドレスや宛先IPアドレス（これらはIPパケットのIPヘッダに付与されている）が重要な鍵となることが多い。従って、所定時間内に取得したIPパケットを送信元IPアドレス及び/又は宛先IPアドレスにより分類して保持することで、それらのIPパケットから攻撃を検知しやすくなる。本発明では、より具体的には、前記攻撃検知手段は、次のように種々様々の攻撃を検知する。まず、クラッカーによる第1の種類の攻撃として、一般にポートスキャン（Port Scan）と言われる種類の攻撃がある。この攻撃は、ネットワークに直接的な損害を及ぼすものではないが、その前段階の攻撃として用いられることが多い。この攻撃では、クラッカーは、自身の管理下にあるホストから、攻撃対象のネットワークに対して、パケット内の宛先IPアドレスや宛先ポート番号を適宜変更しながらIPパケットを繰り返して送信する。そして、それらのIPパケットに対する応答を上記ホストを介して観測することで、攻撃対象のネットワークにおいて、ファイアウォール等による制限を受けずに外部との通信に利用されているIPアドレスやポート番号を探索する。なお、ここで、前記ポート番号は、TCPあるいはUDP上で動作するアプリケーションソフトウェアのサービス種類（例えばtelnet, ftp, smtp, tftp等）を表すもので、IPパケット内のTCPヘッダあるいはUDPヘッダに付与されるデータである。この種の攻撃では、上記のようなIPパケットの送信は、通常、専用のツールソフトウェアを用いて行われ、攻撃対象のネットワークには、宛先IPアドレスやポート番号が互いに異なり、且つ送信元IPアドレスが同一であるようなIPパケットが比較的短時間内に多数、送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のIPパケットであって、少なくともその送信元IPアドレスが互いに同一で且つ宛先IPアドレス又は宛先ポート番号が互いに異なるものが所定時間内に所定数以上取得されたとき、第1の種類の前記攻撃がなされたことを検知する。これにより、ポートスキャンと言われる第1の種類の攻撃を確実に見出すことができる。次に、クラッカーによる第2の種類の攻撃として、一般にSYN FLOODと称される種類の攻撃がある。この攻撃は、TCPの特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、TCPでは二つのホスト間で通信を行う場合、まず、両ホスト間で論理的なコネクションの開設処理が行われる。このコネクション開設処理では、一方のホストから他方のホストに対してSYN用IPパケットを送信する。ここで、該SYN用IPパケットは、それを詳しく言えば、

上記一方のホストのIPアドレスと他方のホストのIPアドレスとをそれぞれ送信元IPアドレス、宛先IPアドレスとしたIPパケットで、そのパケット内のTCPヘッダのSYNビット及びACKビットのうちのSYNビットのみを「1」としたものである。そして、コネクション開設処理では、このSYN用IPパケットを受けた他方のホストは、前記一方のホストに対してSYN/ACK用IPパケットを送信する。ここで、該SYN/ACK用IPパケットは、詳しくは、上記他方のホストのIPアドレスと一方のホストのIPアドレスとをそれぞれ送信元IPアドレス、宛先IPアドレスとしたIPパケットで、そのパケット内のTCPヘッダのSYNビット及びACKビットを共に「1」としたものである。さらに、コネクション開設処理では、このSYN/ACK用IPパケットを受けた前記一方のホストは、前記他方のホストに対してACK用IPパケットを送信し、このACK用IPパケットを前記他方のホストが受けることで、両ホスト間の論理的なコネクションの開設がなされる。なお、上記ACK用IPパケットは、詳しくは、前記SYN用IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットで、そのパケット内のTCPヘッダのSYNビット及びACKビットのうちのACKビットのみを「1」としたものである。前記SYN FLOODは、このようなTCPの特性を利用する攻撃であり、この攻撃では、クラッカーは、攻撃対象のネットワークの特定のホストに対して、比較的短い時間内に多数のSYN用IPパケットを送信する。そして、それらの各SYN用IPパケットに対して上記特定ホストからSYN/ACK用IPパケットが送信されてきても、ACK用IPパケットをその特定ホストに送信しない。このような攻撃がなされたとき、上記特定ホストは、最初に送信されてきたSYN用IPパケットに対するSYN/ACK用IPパケットを送信した後、所定時間（一般に2分）は、その時間内にACK用パケットが送信されてこない限り、そのACK用パケットの受信待ち状態となる。そして、この状態で新たなSYN用パケットが送信されてくる毎に、上記特定ホストは、新たなSYN用パケットに応じたコネクション開設処理を順番に完結すべくその新たなSYN用パケットの情報を通信処理用のバッファ領域に蓄積していく。ところが、バッファ領域の大きさは限界があり、該バッファ領域が満杯になり、このようになると、前記特定ホストは、TCPの通信処理やTCP上のサービス処理を行うことができなくなり、これにより、特定ホストがダウンすることとなる。この種の攻撃（SYN FLOOD）では、前述のように、比較的短い時間内に、比較的多くのSYN用IPパケットが攻撃対象のネットワーク内の特定のホスト（特定のIPアドレスを有するホスト）に対して送信されてくる。また、これに応じて、当該特定のホストからネットワークの外側に向かって、比

較的短い時間内に、多くのSYN/ACK用IPパケットが送信される。さらに、それらのSYN用IPパケットあるいはSYN/ACK用IPパケットに対応して最終的に前記特定ホストに送信されてくべきACK用パケットがその特定ホストに送信されていない。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきたTCPに基づく複数のSYN用IPパケットであって、少なくともその宛先IPアドレスが互いに同一であるものが所定時間内に所定数以上取得され、且つ、その各SYN用IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有すると共に前記TCPに基づくACK用IPパケットが前記所定時間内に取得されなかったとき、第2の種類の前記攻撃がなされたことを検知する。あるいは、前記攻撃検知手段は、前記ネットワークからその外部に送信されたTCPに基づく複数のSYN/ACK用IPパケットであって、少なくともその送信元IPアドレスがそれぞれ互いに同一であるものが所定時間内に所定数以上取得され、且つ、前記TCPに基づくACK用IPパケットであって、前記各SYN/ACK用IPパケットの送信元IPアドレス及び宛先IPアドレスとそれぞれ同一の宛先IPアドレス及び送信元IPアドレスを有するものが前記所定時間内に取得されなかったとき、第2の種類の前記攻撃がなされたことを検知する。これにより、SYN FLOODといわれる第2の種類の攻撃を確実に検知することができる。次に、クラッカによる第3の種類の攻撃として、一般にTeardropと称される種類の攻撃がある。この攻撃は、IPパケットの分轄（所謂IPフラグメント）に係る処理の特性を利用してネットワーク内の特定のホストをダウンさせるものである。すなわち、IPパケットは、インターネット上をルータを介して転送される過程で、各ルータのデータ処理容量の関係上、分轄されることがある。また、各ルータにおいてIPパケットが転送される際にエラーが生じることもあり、このような場合には、ルータは、IPパケットの再送信を行う。このため、IPパケットの宛先IPアドレスのホストでは、分轄された一部の同じIPパケットが、複数受信されるということもある。このようなことから、IPに基づく通信では、最終的にIPパケットを受け取るホスト（宛先IPアドレスのホスト）は、受け取ったIPパケットが分轄されたものであると、残りの全ての分轄部分のIPパケットを受信するまで、各分轄部分のIPパケットを蓄積保持し、全ての分轄部分のIPパケットを受信してから、それらを整理して元のIPパケットのデータを復元する処理を行う。前記Teardropは、このようなIPパケットの分轄に係る処理の特性を利用する攻撃であり、この攻撃では、クラッカーは、比較的短い時間内に、多数の同じ分轄部分のIPパケットを攻撃対象のネットワークの特定のホストに送信した上で、残りの分轄部分のIPパケットをその特

定ホストに送信する。このような攻撃がなされたとき、上記特定ホストは、最終的に残りの分幅部分のIPパケットを受信したときに、そのIPパケットと、先に送信されてきた多量の分割部分のIPパケットとから元のIPパケットのデータを復元しようとする処理を行うため、その処理に長時間を要するものとなる。このため、該特定ホストは、事実上、ダウンしてしまうこととなる。この種の攻撃（Teardrop）では、前述の如く、比較的短い時間内に、多数の同じ分幅部分のIPパケットがネットワーク内の特定のホストに送信されてくる。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数の分割されたIPパケットであって、同一の分割部分が所定時間内に所定数個以上取得されたとき、第3の種類の前記攻撃がなされていることを検知する。これにより、Teardropといわれる第3の種類の攻撃を確実に検知することができる。次に、クラッカーによる第4の種類の攻撃として、一般にLandと称される種類の攻撃がある。この攻撃は、送信元IPアドレス及び宛先IPアドレスが同一であるような、正規にはあり得ないIPパケットを、攻撃対象のネットワークの特定のホストに送信する攻撃である。このようなIPパケットを送信された特定ホストは、そのIPパケットの処理に手間取ることが多く、ダウンしてしまうことがしばしばある。この種の攻撃では、上記の如く、送信元IPアドレス及び宛先IPアドレスが同一であるIPパケットが、ネットワーク内の特定のホストに送信され、しかも、一般には、そのようなIPパケットが比較的短い時間内に、複数、上記特定ホストに送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワークにその外部から送信されてきた複数のIPパケットであって、その送信元IPアドレスが宛先IPアドレスと同一のアドレスとなっているものが所定時間内に所定数個以上取得されたとき、第4の種類の前記攻撃がなされていることを検知する。これにより、Landとされる第4の種類の攻撃を確実に検知することができる。次に、クラッカーによる第5の種類の攻撃として、ネットワーク内の特定のホストのユーザのパスワードを獲得する攻撃がある。この攻撃では、クラッカーは、攻撃対象のネットワーク内の特定のホストのユーザ名を使って、telnet等により上記特定ホストにログインし、さらに所定の辞書ファイルなどから選択した多数のパスワードを使って、その特定ホストの操作を試みる。そして、このとき、その特定ホストの操作ができるか否かにより、パスワードが判明することとなる。この種の攻撃では、同一のユーザ名データを含み、しかも互いに異なるパスワードを有する多数のIPパケットが、攻撃対象のネットワークの特定ホストに送信される。そこで、本発明では、前記攻撃検知手段は、前記ネットワーク内の特定のホストを操作すべく該ネットワークにその外部から送信されてきた複数の

IPパケットであって、前記特定のホストに係るユーザ名データが互いに同一で、且つパスワードが互いに異なるものが所定時間内に所定数以上取得したとき、第5の種類の前記攻撃がなされていることを検知する。これにより、上記のようにパスワードを獲得する攻撃を確実に検知することができる。次に、クラッカーによる第6の種類の攻撃として、ネットワーク内の特定のホストに、ネットワーク管理者など、ごく限られた者が、専用のパスワードを入力した状態でしか実行させることができないような処理（所謂、ルートコマンド）を行わせる攻撃がある。この攻撃は、攻撃対象のホストが搭載しているOS（Operation System）のセキュリティホールといわれるバグを利用するものである。すなわち、例えばUNIXマシン（ホスト）は、バッファオーバーフローといわれるセキュリティホールを有しており、このセキュリティホールは、例えばプリンタの論理名を表す「lpr」というコマンドを含む比較的大きなデータ（128文字以上のデータ）が一度に送られてきたとき、バッファがオーバーフローし、そのオーバーフローしたデータ内に、ルートコマンドがあると、ネットワーク管理者などのパスワードが入力されていくとも、そのルートコマンドを実行してしまうというものである。前記第6の種類の攻撃は、このようなバッファオーバーフローといわれるセキュリティホールを攻撃するもので、前述の「lpr」というコマンドを含む所定サイズ以上のデータ列というような、所定のパターンのデータを含むデータ列を有するIPパケットがネットワークの特定のホストに送信される。そこで、本発明では、前記攻撃検知手段は、バッファオーバーフローと言われるセキュリティホールを攻撃する所定のパターンのデータを有するデータ列を有するIPパケットを取得したとき、第6の種類の前記攻撃がなされていることを検知する。これにより、上記のような第6の種類の攻撃を検知することができる。前述のようにクラッカーによる攻撃を検知する攻撃検知手段を備えた本発明では、前記処理手段が行う処理は、例えば前記攻撃が検知された旨を表す報知出力を発生する処理である。この報知出力の発生により、ネットワーク管理者やあるいは外部の専門技術者等が、検知された攻撃を排除するための処置を施すことが可能となる。

【0006】あるいは、前記処理手段が行う処理は、前記攻撃検知手段が検知した前記攻撃に係る特定の送信元IPアドレス及び/又は宛先IPアドレスを有するIPパケットの前記ネットワークへの進入を阻止する処理である。これにより、クラッカーによるネットワークへの通信、あるいは、攻撃対象とされたホストへの通信が自動的に遮断され、攻撃の検知に応じたネットワークの保護をリアルタイムで図ることができる。より具体的には、ポートスキャンと言われる前記第1の種類の攻撃を検知したときには、前記処理手段が行う処理は、前記攻

撃検知手段が前記第1の種類の攻撃を検知してから所定時間、前記攻撃検知手段が検知した前記第1の種類の攻撃に係る前記送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記送信元IPアドレスが、クラッカーがポートスキャンの攻撃に使用しているホストのIPアドレスであるので、このIPアドレスを送信元IPアドレスとしてネットワークに送信されてくるIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、攻撃が検知されてから所定時間は、上記送信元IPアドレスのホストからネットワークへの通信を行うことができなくなり、ネットワークに関する情報を取得することができなくなる。なお、このとき、ポートスキャンの攻撃が継続的に行われる限り、逐次、それが検知されるので、事実上、その攻撃が継続している間は、事実上、クラッカーは、ネットワークへの通信を行うことができなくなる。また、SYN FLOODといわれる前記第2の種類の攻撃については、この攻撃を前述のようにSYN用IPパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN用IPパケットと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記各SYN用IPパケットの宛先IPアドレスがSYN FLOODの攻撃の対象とされているホストのIPアドレスであるので、そのホストのIPアドレスを宛先IPアドレスとするIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。また、SYN FLOODの攻撃をSYN/ACK用IPパケットに基づいて検知した場合には、前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記各SYN/ACK用IPパケットは、SYN FLOODの攻撃を行おうとしているクラッカーの管理下にあるホストからネットワークに送信されてSYN用IPパケットに対して、ネットワーク内のホストがクラッカー側に応答するパケットであるので、前記各SYN/ACK用IPパケットの送信元IPパケットの送信元IPアドレスが、SYN FLOODの攻撃の対象とされているホストのIPアドレスである。従って、そのネットワーク内のホストのIPアドレスを宛先IPアドレスとして、ネットワークに送信されたIPパケットを該ネットワークに対して遮断する。上記のように、SYN FLOODの攻撃にかかるIPパケットがネットワークに進入するのを阻止することで、その攻撃の対象とされたネットワーク内のホストには、所定時間は、SYN

用IPパケット等のIPパケットが送信されてこなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきたSYN用IPパケットに対してある程度の時間内（通常2分）にコネクション開設を正常に完結することができないと、自動的にコネクション開設の処理を中止する。従って、上記のようにIPパケットが所定時間、送信されてこなくなることで、その所定時間内に正常状態に復帰することができる。さらに、本発明では、SYN FLOODの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN用IPパケットと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含む。あるいは、前記攻撃検知手段が前記第2の種類の攻撃を検知してから所定時間、前記各SYN/ACK用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含む。すなわち、SYN FLOODでは、クラッカーがSYN用IPパケットを送信するに際して、送信元IPアドレスを偽ったり、送信元IPアドレスを適宜変更したりすることもあるが、一般には、前記各SYN用IPパケットの送信元IPアドレス、あるいはそれに対応したSYN/ACK用IPパケットの宛先IPアドレスは、クラッカーの管理下にあるホストのIPアドレスである可能性が高い。従って、このようなIPアドレスを送信元IPアドレスとして有するIPパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。この場合さらに、前記各SYN用IPパケットと同一の送信元IPアドレス、あるいは、前記各SYN/ACK用IPパケットの宛先IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間は、前記SYN用IPパケットと同一の宛先IPアドレス、あるいは、前記各SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間よりも長く設定する。すなわち、SYN FLOODの攻撃対象のホストへの通信を遮断する時間（上記の後者側の所定時間）は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分である。これに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間（上記の前者側の所定時間）は、ネットワークの保護の観点から、比較的に長いものとすることが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側の所定時間よりも長く設定する。これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、SYN FLOODに対するネットワークの保護も十分に図ることができる。

る。また、Teardropといわれる前記第3の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第3の種類の攻撃を検知してから所定時間、前記分割されたIPパケットに係る宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、前記分替されたIPパケットに係る宛先IPアドレスが、Teardropの攻撃の対象とされているホストのIPアドレスであるので、そのホストのIPアドレスを宛先IPアドレスとするIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、Teardropの攻撃の対象とされたネットワーク内のホストには、所定時間は、分替されたIPパケット等のIPパケットが送信されてなくなる。この場合、攻撃対象とされたホストでは、先に送信されてきた分替部分のIPパケットに対応する残りのIPパケットが、ある程度の時間内

(通常1分)に受信されないこと、そのIPパケットに関する通信処理を自動的に中止する。従って、上記のようにIPパケットが所定時間、送信されてなくなることで、その所定時間内に正常状態に復帰することができる。さらに、本発明では、Teardropの検知に応じて、前記処理手段が行う処理は、前記攻撃検知手段が前記第3の種類の攻撃を検知してから所定時間、前記分割されたIPパケットに係る送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理を含む。すなわち、前述したSYN FLOODの場合と同様に、前記分替されたIPパケットに係る送信元IPアドレスは、クラッカーの管理下にあるホストのIPアドレスである可能性が高い。従って、このようなIPアドレスを送信元IPアドレスとして有するIPパケットは、攻撃が検知されてから所定時間はネットワークに対して遮断する。これにより、クラッカーの攻撃に対するネットワークの保護をより高めることができる。この場合さらに、前記分割されたIPパケットに係る送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する前記所定時間より長く設定する。すなわち、SYN FLOODの場合と同様、Teardropの攻撃対象のホストへの通信を遮断する時間(上記の後者側の所定時間)は、該ホストがその攻撃に対して正常に復帰し得る程度の時間で十分であるのに対して、クラッカーの管理下にある可能性の高いホストからネットワークへの通信を遮断する時間(上記の前者側の所定時間)は、ネットワークの保護の観点から、比較的に長いものとするのが好ましいと考えられる。従って、上記の前者側の所定時間を、後者側

の所定時間よりも長く設定する。これにより、ネットワーク内のホストの外部との通信の自由度をできるだけ確保しつつ、Teardropに対するネットワークの保護も十分に図ることができる。

【0007】また、LANDといわれる前記第4の種類の攻撃を検知した場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第4の種類の攻撃を検知してから所定時間、該第4の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、LANDという攻撃では、送信元IPアドレスと宛先IPアドレスとが同一であるIPパケットが送信されてくるので、そのIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、LANDという攻撃からネットワークを保護することができる。また、ネットワーク内のホストのユーザのパスワードを獲得する前記第5の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第5の種類の攻撃を検知してから所定時間、該第5の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、第5の種類の攻撃に係るIPパケットの宛先IPアドレスは、攻撃対象とされたホストのIPアドレスであり、また、該IPパケットの送信元IPアドレスは、クラッカーの管理下にあるホストのIPアドレスである。従って、第5の種類の攻撃に係るIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットを、攻撃が検知されてから所定時間、ネットワークに対して遮断する。これにより、クラッカーは、種々のパスワードを有するIPパケットをネットワークの特定のホストに送信しても、その各パスワードで当該特定ホストを操作することができるのかどうか判断がなくなるので、上記第5の種類の攻撃からネットワークを保護することができる。また、セキュリティホールを利用した前記第6の種類の攻撃を検知する場合にあっては、前記処理手段が行う処理は、前記攻撃検知手段が前記第6の種類の攻撃を検知してから所定時間、該第6の種類の攻撃に係る前記IPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットが前記ネットワークに進入するのを阻止する処理である。すなわち、第6の種類の攻撃に係るIPパケットの宛先IPアドレスは、攻撃対象とされたホストのIPアドレスであり、また、該IPパケットの送信元IPアドレスは、クラッカーの管理下にあるホストのIPアドレスである。従って、第6の種類の攻撃に係るIPパケットと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットを、攻撃が検知されて

から所定時間、ネットワークに対して遮断する。これにより、クラッカーは、ネットワーク内の特定のホストセキュリティホールを攻撃するIPパケットをネットワークの特定のホストに送信しても、該IPパケットは、当該特定ホストに与えられなくなるので、当該特定ホストにルートコマンドを実行させることができなくなり、前記第6の種類の攻撃からネットワークを保護することができる。以上説明したように各種の攻撃に係るIPパケットのネットワークへの進入を、攻撃の検知に応じて自動的に行う本発明では、前記ネットワークの入り口に、該ネットワークに進入を阻止するIPパケットを選択的に設定可能なパケットフィルタを設けておき、前記処理手段は、前記処理を該パケットフィルタを制御することにより行う。これによれば、前記パケットフィルタとして、例えばファイヤウォールを用いることで、既存のシステムを流用しつつ本発明のシステムを構築することが可能となる。なお、ファイヤウォールよりもIPパケットの取捨・選択の機能は劣るが、一般にルータもパケットフィルタとしての機能を有しており、従って、前記パケットフィルタとしてルータを用いることも可能である。

#### 【発明の実施の形態】

【0008】本発明の一実施形態を図1を参照して説明する。図1は本実施形態のシステム構成図である。図1において、1はネットワークとしてのLANである。このLAN1は、例えばイーサネット(Ethernet)を用いて構築されたものであり、図示を省略する複数のホスト(コンピュータ)がイーサネット・ケーブルやハブ等を介して接続されている。各ホストには、それをイーサネット・ケーブルに接続するイーサネット・カードや、TCP/IPの処理を行うためのソフトウェア、TCP/IP上で機能する各種アプリケーションソフトウェア(例えば、telnet、ftp、smtp等)が実装され、IPに基づく通信を可能としている。なお、LAN1は、イーサネット上で構築されたものに限らず、トークリング等、他の形態で構築されたものであってもよい。本実施形態のシステムでは、LAN1の入り口に、パケットフィルタとしてのファイヤウォールの機能をもたせたコンピュータ2(以下、このコンピュータ2を単にファイヤウォール2と称する)が設けられており、LAN1はファイヤウォール2を介してインターネット3に接続されている。ファイヤウォール2は、どのような種類のIPパケットのLAN1への進入を禁止するかを規定するデータが書き込まれるファイル(以下、フィルタ設定ファイルという)を有しており、このフィルタ設定ファイルで、LAN1への進入が禁止された種類のIPパケットがインターネット3側から送信されてきたときに、そのIPパケットを廃棄してLAN1への進入を阻止する。そして、フィルタ設定ファイルで、LAN1への進入が禁止されていないIPパケッ

トが送信されてきたときには、それをLAN1に転送する。ファイヤウォール2とインターネット3との間には、ハブ4が介装され、このハブ4に攻撃検知手段の機能をもたせたセンサ5が接続されている。また、このセンサ5には、前記ファイヤウォール2を制御する処理手段の機能を有するディレクタ6が接続されている。これらのセンサ5及びディレクタ6はそれらコンピュータにより構成されたものである。前記センサ5は例えばUNIXマシンにより構成され、イーサネットカード7を介して前記ハブ4に接続されている。この場合、センサ5には、TCP DUMPといわれるソフトウェアが実装されており、このTCP DUMPによって、ハブ4を通る全てのIPパケットをイーサネットカード7を介して取得する(ヒアリングする)ことができるようになっている。そして、センサ5は、取得した各IPパケットをその取得時点の時刻データと共に図示しないハードディスクに記憶保持するようにしている。なお、ハードディスクに記憶保持したIPパケットの総量が所定の許容量に達したときには、センサ5は、最も古いIPパケットを消去し、新たに取得されたIPパケットをハードディスクに記憶保持する。また、センサ5は、IPアドレスを持たず、ARP(Address Resolution Protocol)や、RARP(Reverse Address Resolution Protocol)のパケット等、応答を促すパケットが送信されてきても、それに対する応答をしないようにソフトウェア的に設定されており、IPパケットの受信(取り込み)のみを行うことのできるものとされている。さらに、センサ5には、前述した第1〜第6の種類の攻撃を検知するためのソフトウェア(以下、攻撃検知アルゴリズム)が実装されている。なお、この攻撃検知アルゴリズムは、ディレクタ6に実装しておき、該ディレクタ6とのデータ授受を行いつつ該攻撃検知アルゴリズムの処理をセンサ5に行わせるようにしてもよい。前記ディレクタ6には、前記ファイヤウォール2を制御するソフトウェア(以下、フィルタ制御アルゴリズムという)が実装されている。この場合、フィルタ制御アルゴリズムは、センサ5により検知される攻撃に応じて、前記フィルタ設定ファイルのデータを適宜書き換えることで、前記ファイヤウォール2を制御するものである。次に、かかる本実施形態の作動を説明する。前記センサ5は、取得されるIPパケットを前述の如くハードディスクに記憶保持しつつ、所定のサイクルタイム毎に次のような処理を行う。すなわち、センサ5は、ハードディスクから所定の時間間隔分の複数のIPパケットを、送信元IPアドレス及び宛先IPアドレスの値別に分類(ソート)した上で、図示しないメモリに取り込んで保持する。つまり、所定の時間間隔分の複数のIPパケットのうち、同一の送信元IPアドレスを有するものをひとまとめと

にして、メモリに取り込む（以下の説明では、このようにひとまとめにされたIPパケットの組をIPパケット群という）。そして、このメモリに取り込んだ複数のIPパケットに対して、後述する攻撃検知の処理を行った上で、これらのIPパケットをメモリから消去する。この場合、各サイクルタイムにおいて、メモリに取り込むIPパケットは、前回のサイクルタイムでメモリに取り込んだIPパケットのうちの最も古いIPパケットの取得時刻から所定時間を経過した時刻以後に取得されたものである。各サイクルタイムにおけるセンサ5による攻撃検知の処理は、攻撃検知アルゴリズムに従って次のように行われる。センサ5は、まず、前記第1〜第6の種類の攻撃のうち、例えば、第1の種類の攻撃、すなわちポートスキャンを検知する処理を行う。この処理では、センサ5は、メモリに前述のように取り込んだIPパケットのうち、送信元IPアドレスが同一で、且つ該送信元IPアドレスがLAN1の外部のものである各IPパケット群に対し、その各IPパケット群に含まれるIPパケットが有する全ての宛先IPアドレスの値（これはLAN1に属するIPアドレスの値である）を抽出する。そして、上記の各IPパケット群で抽出した宛先IPアドレスの各値に対し、そのIPパケット群（同一の送信元IPアドレスのIPパケット群）から、該宛先IPアドレスの値と同一の宛先IPアドレスを有し、且つTCPヘッダあるいはUDPヘッダ内の宛先ポート番号が互いに異なり、且つ、連続した所定時間内（例えば30秒内）に取得されたIPパケットの個数をカウントする。このとき、このカウント数が所定数（例えば20個）に達した場合には、センサ5は、ポートスキャンの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたIPパケット群の送信元IPアドレスの値データとを（以下、これらのデータを第1種攻撃検知データという）前記ディレクタ6に与える。このような処理が送信元IPアドレスが同一で、且つ該送信元IPアドレスがLAN1に属さない全てのIPパケット群に対し順次行われる。なお、本実施形態におけるポートスキャンの検知では、ポート番号が互いに異なるIPパケットの個数をカウントするようにしたが、次のような処理によりポートスキャンを検知するようにしてもよい。すなわち、送信元IPアドレスが同一で、且つ、該送信元IPアドレスがLAN1外部のものである各IPパケット群に対し、その各IPパケット群に含まれるIPパケットが有する全ての宛先ポート番号の値を抽出し、その抽出した宛先ポート番号の各値に対し、該宛先ポート番号を抽出したIPパケット群から、該宛先ポート番号の値と同一の宛先ポート番号を有し、且つ宛先IPアドレスが互いに異なり、且つ、連続した所定時間内に取得されたIPパケットの個数をカウントする。そして、そのカウント数が所定数に達した場合にポートスキャンが行われていることを検知する。一方、

センサ5から前述のような第1種攻撃検知データを与えられた前記ディレクタ6は、該第1種攻撃検知データに含まれる送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（例えば5分間）阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。このとき、ファイアウォール2は、上記送信元IPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、ポートスキャンの攻撃からLAN1が保護される。なお、ディレクタ6は、上記所定時間（5分間）が経過するまでの間に、先に与えられた第1種攻撃検知データと同一の第1種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間（5分間）、該第1種攻撃検知データの送信元IPアドレスからのIPパケットのLAN1への進入を阻止するようにファイアウォール2を制御する。従って、ポートスキャンの攻撃が続いている限り、その送信元IPアドレスからのIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、上記所定時間（5分間）が経過するまでに、前記第1種攻撃検知データが与えられなかった場合には、その第1種攻撃検知データの送信元IPアドレスからのIPパケットのLAN1への進入の阻止を解除する。前述のようにポートスキャンの攻撃の検知処理を行ったセンサ5は、次に、第2の種類の攻撃（SYN FLOOD）の検知処理を行う。この処理では、センサ5は、宛先IPアドレスが同一であるIPパケット群のうち、LAN1に属する宛先IPアドレスの各IPパケット群に対し、該IPパケット群に含まれるSYN用IPパケットをその取得時刻順に順次抽出する。そして、抽出した各SYN用IPパケットの取得時刻から所定時間（例えば2秒間）内に取得されたSYN用IPパケットが、同じ宛先IPアドレスのIPパケット群内に存在するか否か調べ、存在する場合には、先に抽出したSYN用IPパケットを含めてそれらのSYN用IPパケットの個数をカウントする。さらに、そのカウントしたそれぞれのSYN用IPパケットに対して、それぞれに対応するACK用IPパケット（詳しくは該SYN用IPパケットと同一の送信元IPアドレスを有し、且つ、該SYN用IPパケットのTCPヘッダ中のシーケンス番号の次のシーケンス番号を有するACK用IPパケット）であって、且つ該SYN用IPパケットの取得時刻から上記所定時間（2秒間）内に取得されたものが、同じ宛先IPアドレスのIPパケット群内に存在するか否かを調べ、存在する場合には、その都度、上記のカウント数を「1」ずつ減少させる。そして、最終的に、対応するACK用IPパケットの存在を調べ終わったときに上記のカウント数が所定数（例えば16個）以上である場合には、SYN FLOODの攻撃がなされていることを検知し、そのことを

示すデータと、この攻撃が検知されたSYN用IPパケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データとを、(以下、これらのデータを第2種攻撃検知データという)前記ディレクタ6に与える。このような処理が宛先IPアドレスが同一で、且つ該宛先IPアドレスがLAN1に属する全てのIPパケット群に対して順次行われる。なお、本実施形態では、SYN用IPパケットの個数に基づいてSYN FLOODを検知したが、次のような処理によりSYN FLOODを検知するようによい。すなわち、送信元IPアドレスが同一で且つ、該送信元IPアドレスがLAN1に属する各IPパケット群に対し、該IPパケット群に含まれるSYN/ACK用IPパケットをその取得時刻順に順次抽出する。そして、抽出した各SYN/ACK用IPパケットの取得時刻から所定時間(例えば2秒間)内に取得されたSYN/ACK用IPパケットが、同じ送信元IPアドレスのIPパケット群内に存在するか否かを調べ、存在する場合には、先に抽出したSYN/ACK用IPパケットを含めてそれらのSYN/ACK用IPパケットの個数をカウントする。さらに、そのカウントしたそれぞれのSYN/ACK用IPパケットに対して、該SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスのIPパケット群を調べ、該SYN/ACK用IPパケットに対応するACK用IPパケット(詳しくは該SYN/ACK用IPパケットの送信元IPアドレスと同一の宛先IPアドレスを有し、且つ、該SYN/ACK用IPパケットのTCPヘッダ中のシーケンス番号の次のACK番号を有するACK用IPパケット)であって、且つ該SYN/ACK用IPパケットの取得時刻から上記所定時間(2秒間)内に取得されたものが、当該IPパケット群内に存在するか否かを調べる。そして、そのようなACK用IPパケットが存在する場合には、その都度、上記のカウント数を「1」ずつ減少させる。そして、最終的に、対応するACK用IPパケットの存在を調べ終わったときに上記のカウント数が所定数(例えば16個)以上である場合には、SYN FLOODの攻撃がなされていることを検知する。なお、この場合にセンサ5からディレクタ6に与えるデータは、SYN FLOODの攻撃を検知した示すデータと、上記SYN/ACK用IPパケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データである。この場合、SYN/ACK用IPパケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データは、それぞれ、先に説明した前記第2種攻撃検知データにおけるSYN用IPパケット宛先IPアドレスの値データ、送信元IPアドレスの値データに相当するものである。一方、センサ5から前述のような第2種攻撃検知データを与えられた前記ディレクタ6は、該第2種攻撃検知データに含まれる送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットがL

AN1に進入するのを現在から所定時間(例えば2分間)阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。同時に、ディレクタ6は、第2種攻撃検知データに含まれる宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間(例えば2秒間)阻止するようにファイアウォール2のフィルタ設定ファイルを書き換える。このとき、ファイアウォール2は、上記送信元IPアドレスを有するIPパケット、あるいは上記宛先IPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、SYN FLOODの攻撃からLAN1が保護されると共に、この攻撃の対象とされていたIPアドレスのホストがダウンせずに正常状態に復帰することができる。なお、ポートスキヤンの検知時の場合と同様、ディレクタ6は、第2種攻撃検知データにおける送信元IPアドレスを有するIPパケットの排除に係る上記所定時間(2分間)が経過するまでの間に、先に与えられた第2種攻撃検知データと同一の第2種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間(2分間)、該第2種攻撃検知データの送信元IPアドレスからのIPパケットのLAN1への進入を阻止するようにファイアウォール2を制御する。このことは、第2種攻撃検知データにおける宛先IPアドレスを有するIPパケットの排除についても同様である。従って、SYN FLOODの攻撃が続いている限り、その攻撃に係る送信元IPアドレスからのIPパケット、あるいはその攻撃に係る宛先IPアドレスへのIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、第2種攻撃検知データにおける送信元IPアドレスを有するIPパケットの排除と、第2種攻撃検知データにおける宛先IPアドレスを有するIPパケットの排除とのいずれについても、それぞれに対応する上記所定時間(2分間、2秒間)が経過するまでに、前記第2種攻撃検知データが与えられなかった場合には、その第2種攻撃検知データの送信元IPアドレスを有するIPパケット、あるいは、第2種攻撃検知データの宛先IPアドレスを有するIPパケットのLAN1への進入の阻止を解除する。前述のようにSYN FLOODの攻撃の検知処理を行ったセンサ5は、次に、第3の種類の攻撃(Teardrop)の検知処理を行う。この処理では、センサ5は、宛先IPアドレスが同一であるIPパケット群のうち、LAN1に属する宛先IPアドレスの各IPパケット群に対し、該IPパケット群に含まれる分替されたIPパケット(以下、単に、分替パケットという)を順次抽出する。この場合、IPで、分替パケットは、そのIPヘッダ中の特定のフラグが「1」となっているか、もしくは、フラグメントオフセットといわれるデータが「0」より大きな値となっており、これに

より、分轄パケットを見出すことができる。そして、センサ5は、抽出した各分轄パケットの取得時刻から所定時間（例えば5分間）内に取得され、且つ、該分轄パケットとIPヘッダ中のIP識別番号及びフラグメントオフセットの値がそれぞれ同一であるもの（抽出した分轄パケットと同一の分轄パケット）が、該分轄パケットと同じIPパケット群内にあるかを調べる。このとき、そのような分轄パケットがある場合には、先に抽出した分轄パケットを含めてそれらの分轄パケットの個数をカウントする。そして、このカウント数が所定数（例えば80個）以上である場合には、Teardropの攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知された分轄パケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データとを（以下、これらのデータを第3種攻撃検知データという）前記ディレクタ6に与える。このような処理が宛先IPアドレスが同一で、且つ該宛先IPアドレスがLAN1に属する全てのIPパケット群に対して順次行われる。一方、センサ5から前述のような第3種攻撃検知データを与えられた前記ディレクタ6は、前記SYN FLOODが検知された場合と全く同じやり方で、ファイアウォール制御する。すなわち、第3種攻撃検知データに含まれる送信元IPアドレスと同一の送信元IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（2分間）阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。同時に、第3種攻撃検知データに含まれる宛先IPアドレスと同一の宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（2秒間）阻止するようにファイアウォール2のフィルタ設定ファイルを書き換える。これにより、Teardropの攻撃からLAN1が保護されると共に、この攻撃の対象とされていたIPアドレスのホストがダウンせずに正常状態に復帰することができる。上記のようにTeardropの攻撃の検知処理を行ったセンサ5は、次に、第4の種類の攻撃（LAND）の検知処理を行う。この処理では、センサ5は、宛先IPアドレスが同一であるIPパケット群のうち、LAN1に属する宛先IPアドレスの各IPパケット群から、該IPパケット群の宛先IPアドレスと同じ値の送信元IPアドレスを有するIPパケットを抽出する。さらに、その抽出したIPパケットと同じ宛先IPアドレスのIPパケット群の中から、該IPパケットと同じ送信元IPアドレスを有し、且つ該IPパケットの取得時刻から所定時間（例えば2分間）内に取得されたIPパケットが存在するか否かを調べる。そして、そのようなIPパケットが存在する場合には、先に抽出したIPパケットを含めてそれらのIPパケットの該IPパケットの個数をカウントする。このとき、該カウント数が所定数（例えば6個）以上である場合には、LANDの攻撃がなされていることを検知し、そのことを示

すデータと、この攻撃が検知されたIPパケットの送信元IPアドレスの値データを（以下、これらのデータを第4種攻撃検知データという）前記ディレクタ6に与える。このような処理が宛先IPアドレスが同一で、且つ該宛先IPアドレスがLAN1に属する全てのIPパケット群に対して順次行われる。一方、センサ5から前述のような第4種攻撃検知データを与えられた前記ディレクタ6は、第4種攻撃検知データに含まれる送信元IPアドレスと同一の送信元IPアドレスを有し、且つ、該送信元IPアドレスと同一の宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（例えば5分間）阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。このとき、ファイアウォール2は、上記送信元IPアドレス及び宛先IPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、LANDの攻撃からLAN1が保護される。この場合、ポートスキヤクの検知時の場合と同様、ディレクタ6は、第4種攻撃検知データにおける送信元IPアドレスと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットの排除に係る上記所定時間（5分間）が経過するまでの間に、先に与えられた第4種攻撃検知データと同一の第4種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間（5分間）、該第4種攻撃検知データの送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入を阻止するようにファイアウォール2を制御する。従って、LANDの攻撃が続いている限り、その攻撃に係る送信元IPアドレス及び宛先IPアドレスを有するIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、上記所定時間（5分間）が経過するまでに、前記第4種攻撃検知データが与えられなかった場合には、その第4種攻撃検知データの送信元IPアドレスと同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入の阻止を解除する。【0009】なお、本実施形態では、第4種攻撃検知データとして、LANDの攻撃に係るIPパケットの送信元IPアドレスの値データをディレクタ6に与えるようにしたが、LANDの攻撃に係るIPパケットの送信元IPアドレスと、宛先IPアドレスとは同じ値であるので、その送信元IPアドレスの値データの代わりに、宛先IPアドレスの値をディレクタ6に与えてもよいことはもちろんである。前述のように、LANDの攻撃の検知処理を行ったセンサ5は、次に第5の種類の攻撃（パワードの獲得）を検知する処理を行う。この処理では、センサ5は、宛先IPアドレスが同一であるIPパケット群のうち、LAN1に属する宛先IPアドレスの各IPパケット群に対し、LAN1のホストのユーザ名データ及びパスワードデータを含むIPパケットを抽出

する。それらの抽出したIPパケットの中から、ユーザ名データが同一で、且つ、パスワードデータが互いに異なり、且つ、連続した所定時間（例えば2分間）内に取得されたIPパケットの個数をカウントする。このとき、このカウント数が所定数（例えば20個）以上であれば、クラッカーがパスワードを獲得するための第5の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたIPパケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データとを（以下、これらのデータを第5種攻撃検知データという）前記ディレクタ6に与える。このような処理が宛先IPアドレスが同一で、且つ該宛先IPアドレスがLAN1に属する全てのIPパケット群に対して順次行われる。一方、センサ5から前述のような第5種攻撃検知データを与えられた前記ディレクタ6は、該第5種攻撃検知データの送信元IPアドレス及び宛先IPアドレスとそれぞれ同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（例えば1時間）阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。このとき、ファイアウォール2は、上記送信元IPアドレス及びIPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、パスワードの獲得を狙った第5の種類の攻撃からLAN1が保護される。なお、ポートスキャンの検知時の場合と同様、ディレクタ6は、第5種攻撃検知データにおける送信元IPアドレス及び宛先IPアドレスを有するIPパケットの排除に係る上記所定時間（1時間）が経過するまでの間に、先に与えられた第5種攻撃検知データと同一の第5種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間（1時間）、該第5種攻撃検知データの送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入を阻止するようにファイアウォール2を制御する。従って、第5の種類の攻撃が続いている限り、その攻撃に係る送信元IPアドレス及び宛先IPアドレスを有するIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、上記所定時間（1時間）が経過するまでに、前記第5種攻撃検知データが与えられなかった場合には、その第5種攻撃検知データの送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入の阻止を解除する。以上説明したようにして、本実施形態のシステムによれば、センサ5や、ディレクタ6を導入するだけで、クラッカーによるLAN1への各種の攻撃をリアルタイムで検知しつつ、検知された攻撃からLAN1を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮してLAN1を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、ひいては、LAN1の維持管理のコストを低減することができる。また、クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、LAN1と外部との通信を格別制限する必要性が少なくなる。このため、通常時は、LAN1の通信の自由度

あるIPパケットを検索する。そして、そのようなIPパケットが見つかった場合には、LAN1のホストのルーローを攻撃する第6の種類の攻撃がなされていることを検知し、そのことを示すデータと、この攻撃が検知されたIPパケットの送信元IPアドレスの値データ及び宛先IPアドレスの値データとを（以下、これらのデータを第6種攻撃検知データという）前記ディレクタ6に与える。一方、センサ5から前述のような第6種攻撃検知データを与えられた前記ディレクタ6は、該第6種攻撃検知データの送信元IPアドレス及び宛先IPアドレスとそれぞれ同一の送信元IPアドレス及び宛先IPアドレスを有するIPパケットがLAN1に進入するのを現在から所定時間（例えば6時間）阻止するように前記ファイアウォール2のフィルタ設定ファイルを書き換える。このとき、ファイアウォール2は、上記送信元IPアドレス及びIPアドレスを有するIPパケットがインターネット3から送信されてくると、そのIPパケットを廃棄し、LAN1への進入を阻止する。これにより、LAN1のホストのルーローを攻撃する第6の種類の攻撃からLAN1が保護される。なお、ポートスキャンの検知時の場合と同様、ディレクタ6は、第6種攻撃検知データにおける送信元IPアドレス及び宛先IPアドレスを有するIPパケットの排除に係る上記所定時間（6時間）が経過するまでの間に、先に与えられた第6種攻撃検知データと同一の第5種攻撃検知データがセンサ5から再度与えられれば、その時点から上記所定時間（6時間）、該第6種攻撃検知データの送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入を阻止するようにファイアウォール2を制御する。従って、第6の種類の攻撃が続いている限り、その攻撃に係る送信元IPアドレス及び宛先IPアドレスを有するIPパケットは、LAN1に進入することはできない。そして、ディレクタ6は、上記所定時間（6時間）が経過するまでに、前記第6種攻撃検知データが与えられなかった場合には、その第5種攻撃検知データの送信元IPアドレス及び宛先IPアドレスを有するIPパケットのLAN1への進入の阻止を解除する。以上説明したようにして、本実施形態のシステムによれば、センサ5や、ディレクタ6を導入するだけで、クラッカーによるLAN1への各種の攻撃をリアルタイムで検知しつつ、検知された攻撃からLAN1を保護する適正な処置を自動的に迅速に施すことができる。このため、ネットワーク管理者等は、クラッカーによる攻撃を考慮してLAN1を構築したり、頻繁にログファイルを参照したりする労力が大幅に削減され、ひいては、LAN1の維持管理のコストを低減することができる。また、クラッカーによる各種攻撃をリアルタイムで検知できることから、攻撃が検知されない状況では、LAN1と外部との通信を格別制限する必要性が少なくなる。このため、通常時は、LAN1の通信の自由度

を高めることができ、インターネット3上の情報資源を有効に活用することができる。なお、以上説明した実施形態では、LAN1の入り口にファイヤウォール3を設けておき、クラッカーによる攻撃が検知されたとき、該ファイヤウォール3を制御することで、検知された攻撃を自動的に排除する処置を行ったが、クラッカーによる攻撃が検知されたときに、単に、その旨の報知をネットワーク管理者や、専門の警備管理者等に行うようにしてもよい。この場合には、例えば前記ディレクタ6あるいはセンサ5を公衆回線や専用回線を介してネットワーク管理者や、警備管理者等のホストに接続しておく。そして、攻撃が検知された場合に、前述した第1乃至第6種攻撃検知データのような情報をネットワーク管理者や警備管理者等のホストにディレクタ6あるいはセンサ5から

\*ら送信する。このようにしたときには、検知された攻撃からLAN1を保護するための具体的な処置は、ネットワーク管理者等が直接的に行うこととなる。しかるに、この場合であっても、ネットワーク管理者等は、上記の報知を受けたときに処置を施せばよく、しかも攻撃の種類は検知されるので、攻撃に対する処置を比較的容易に施すことができる。

#### 【図面の簡単な説明】

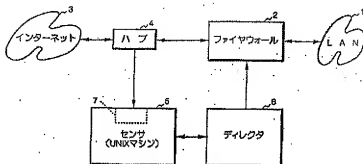
【図1】本発明のクラッカー監視システムの一実施形態のシステム構成図。

#### 【符号の説明】

1…LAN（ネットワーク）、2…ファイヤウォール（パケットフィルタ）、5…センサ（攻撃検知手段）、6…ディレクタ（処理手段）。

【図1】

（四）



フロントページの続き

(51) Int. Cl.<sup>7</sup>

H04L 12/56

識別記号

FI

テーマコード（参考）